あらゆるログの収集と保管
Active Directory監査
機械学習を使用した異常検知

スタートアップガイド

ManageEngine

Log360

2022年 11月 15日 改訂

■著作権について
本ガイドの著作権は、ゾーホージャパン株式会社が所有しています。
■注意事項
本ガイドの内容は、改良のため、予告なく変更することがあります。ゾーホージャパン株式会社は本ガイドに関しての一切の責任を負いかねます。 当社はこのガイドを使用することにより引き起こされた偶発的もしくは間接的な損害についても責任を負いかねます。

■商標一覧
OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。
Windows は、米国およびその他の国における米国Microsoft Corp. の登録商標です。
ManageEngine は、ZOHO Corporation Pvt.Ltd社の登録商標です。
なお、本ガイドでは、(R)、TM表記を省略しています。

目次

1. はじめに

1-1 本ガイドについて

本ガイドではLog360およびLog360 UEBAのインストール方法について説明します。

1-2 対象読者

本ガイドは、Log360およびLog360 UEBAを導入するシステム管理者を対象としています。

1-3 Log360の概要

ManageEngine Log360は、当社製品「**ADAudit Plus**」「**EventLog Analyzer**」を1つのコンソール画面で管理できる製品です。両製品を1つのコンソール画面で管理することで、ネットワークセキュリティとActive Directoryの監査が容易になります。

- **ADAudit Plus**
  Active Directoryログの可視化およびアラート通知を行う監査ツール

- **EventLog Analyzer**
  あらゆるログを一括管理する統合ログ管理ツール

1-4 オプション

Log360はオプションとして、Microsoft 365監査が容易になる「**M365 Manager Plus**」、および、機械学習のアルゴリズムを活用してネットワーク上のユーザー/デバイスの異常行動を検知する「**Log360 UEBA**」を使用できます。Log360をインストールしてから30日間は両製品とも無料で利用できます。30日が経過すると自動的に無料版へ移行します。

※Log360のオプションとして「M365 Manager Plus」を使用する場合、ユーザー管理機能が使用できません。

1-5 ライセンスの種類

ManageEngine製品には「通常ライセンス」と「年間ライセンス」の2つのライセンス形態があります。各ライセンス形態の特徴とメリットは以下のとおりです。

通常ライセンスと年間ライセンスの比較

種類	特徴	メリット
通常ライセンス	● 無期限の製品ライセンスに、初年度のみの年間保守サポートサービスが含まれている ● 製品の納品日から保守サービスが開始され、以後、1年ごとに年間保守サポートサービス契約を更新する	半永久的に利用可能
年間ライセンス	● 1年間利用可能な製品ライセンスで、年間保守サポートサービスが含まれている ● 1年ごとに年間ライセンス契約を更新する	少額の費用で 利用開始可能

1-6 評価版から購入版にアップグレードする方法

1. Log360にログイン後、画面の右上にある[ライセンス]をクリックします。

2. ポップアップ画面下部の[参照]をクリックして、購入したライセンスファイルを選択します。
3. [ライセンスの使用許諾を申請する]をクリックすることで、ライセンスが適用されます。
4. ライセンスを適用後、製品のデフォルト管理者アカウント（admin）およびデフォルト技術者アカウント（operator）のパスワード変更を要求する通知が表示されますので、[すぐに変更する]をクリックします。

5. adminについて、「現在のパスワード」に「admin」と入力します。「新しいパスワード」および「パスワードを確認する」に任意のパスワードを入力します。
6. operatorについて、「新しいパスワード」および「パスワードを確認する」に任意のパスワードを入力します。

7. [パスワードを変更する]をクリックします。

2. システム要件

2-1 最小ハードウェア要件

Log360のみを利用した場合（EventLog AnalyzerやADAudit Plusなどのコンポーネント製品を含まない）の最小要件は以下のとおりです。

- CPU: 2.4 GHz / 2 コア
- メモリー（RAM）: 8 GB 以上
- ハードディスク: 60 GB 以上

製品パフォーマンスの観点より、原則、各コンポーネント製品毎に専用のサーバーをご用意いただくことを推奨します。各製品におけるハードウェア要件は各製品のページをご参照ください。

各製品のハードウェア要件

- EventLog Analyzer
- ADAudit Plus
- M365 Manager Plus
- Log360 UEBA

なお、各製品毎にサーバーを用意できない場合、以下例のように2つのサーバーをご用意いただけます。

例）

- サーバー1: Log360/EventLog Analyzer/ADAudit Plusをインストール
- サーバー2: M365 Manager Plus/Log360 UEBAをインストール

上記例のように各製品をインストールした場合の最小ハードウェア要件は以下のとおりです。

サーバー1の最小ハードウェア要件

- CPU: 2.4 GHz / 16 コア
- メモリー（RAM）: 52 GB 以上
- ハードディスク: 1.5 TB 以上

サーバー2の最小ハードウェア要件

- CPU: 2.4 GHz / 6 コア
- メモリー（RAM）: 24 GB 以上
- ハードディスク: 200 GB 以上

※製品導入の前に、実運用環境またはそれと同等の環境で、十分に製品を評価していただき、利用用途、要件、利用環境に適合することを確認してください。また、導入前にこちらのページを必ずご確認ください。

2-2 サポートOS

- Windows 8 (8.1) / 10
- Windows Server 2012 / 2012 R2 / 2016 / 2019

※クライアント OS は評価目的でのみ利用可能です。本番環境にはサーバーOS をご利用ください。

2-3 サポートWebブラウザー

- Google Chrome 45 以上
- Mozilla Firefox 40 以上
- Microsoft Edge (Chromium 版)

3. ポート要件

Log360のポート要件

Log360は以下のポートを使用します。

ポート番号	プロトコル	サービス
8095	HTTP	Webサーバー
8458	HTTPS	Webサーバー
25	TCP	SMTP
465	TCP	SMTP (SSL)
587	TCP	SMTP (TLS)
3268	TCP	Global Catalog
3269	TCP	Global Catalog (SSL)
53	TCP/UDP	DNS
67,68	UDP	DHCP
88	TCP/UDP	Kerberos
135	TCP/UDP	DCOM,RPC
49152–65535	TCP	RPC
445	TCP/UDP	WMI

137–139	TCP/UDP	NetBIOS
389	TCP/UDP	LDAP
636	TCP	LDAPS
33335	TCP	PostgreSQL
513,514	UDP	SysEvtCol

各製品のポート要件は各製品のページをご参照ください。

各製品のポート要件

- EventLog Analyzer
- ADAudit Plus
- M365 Manager Plus

4. 評価版インストーラーをダウンロード

評価版インストーラーをこちらのURLよりダウンロードできます。

ダウンロード時から30日間は、評価版として各製品の全ての機能が利用できます。30日の評価期間が終了後は、自動的に無料版に移行します。評価版と無料版の違いの詳細は以下の内容または遷移先ページをご参照ください。

【評価版と無料版の違い】

- EventLog Analyzer
- ADAudit Plus
- M365 Manager Plus: 無料版に移行後、1テナント/25ユーザーの監査が可能です。
- Log360 UEBA: 新たにオプションライセンスの購入が必要です。

5. Log360のインストール手順

インストール手順を説明します。以下3つの場合に分けて説明します。

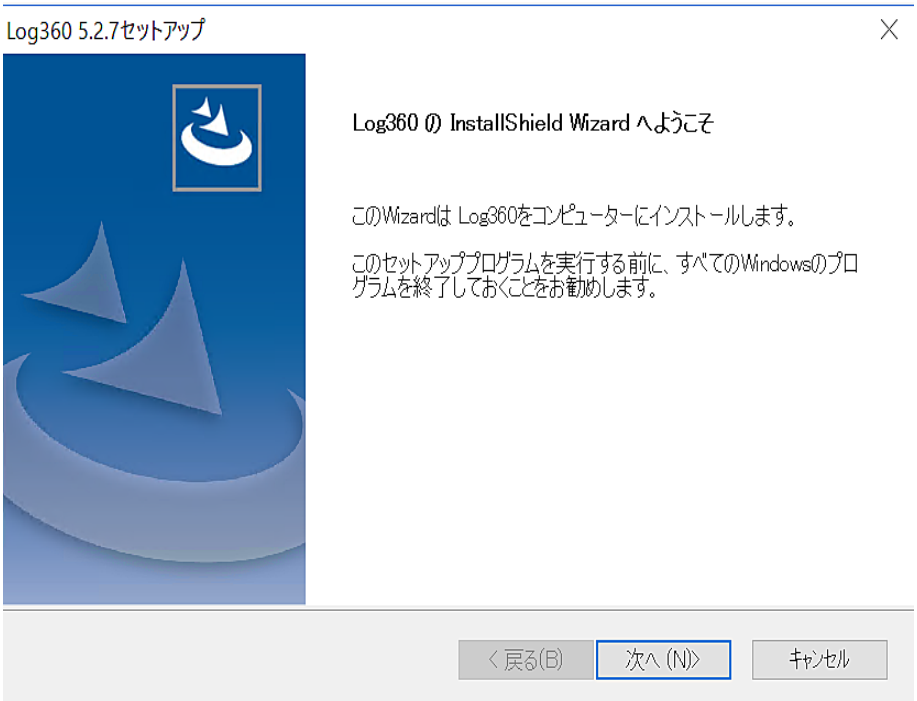
- 5-1 すべての製品を1つのサーバーにインストールする場合
- 5-2 製品を2つのサーバーにインストールする場合
  例）
  サーバー1: Log360/EventLog Analyzer/ADAudit Plus
  サーバー2: M365 Manager Plus/Log360 UEBA

- 5-3 Log360のみをインストールする場合

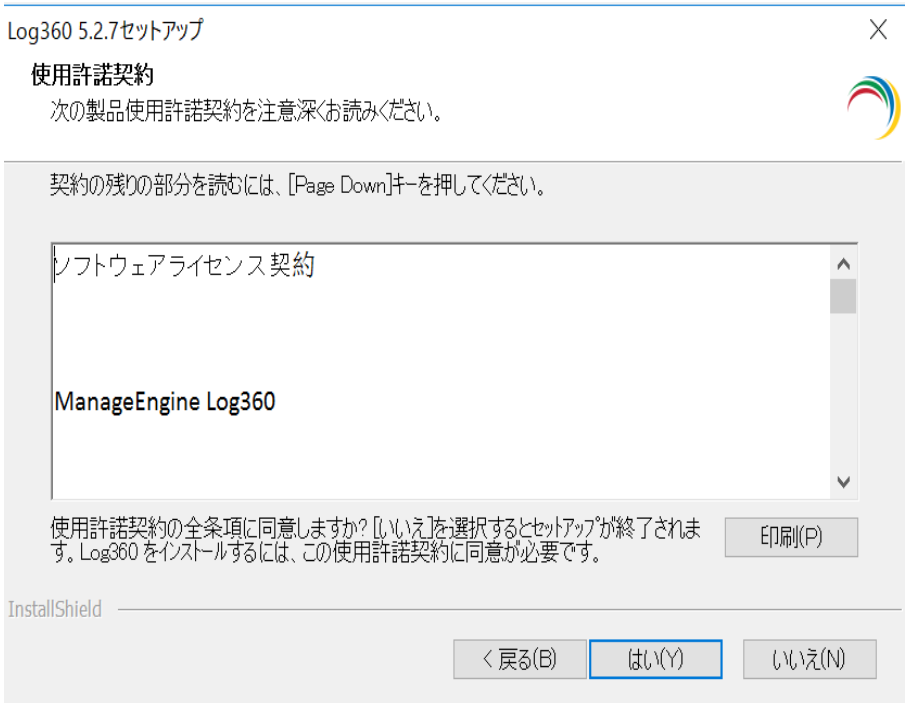
※アンチウイルスソフトやバックアップツールをインストールしている場合
Log360およびコンポーネント製品ををインストールしたフォルダーを、スキャン対象またはバックアップ対象から必ず除外してください。除外しない場合、スキャンまたはバックアップによってデータベースが破損する可能性があります。

5-1 すべての製品を1つのサーバーにインストールする場合

1. 「ManageEngine_Log360_64bit.exe」を管理者権限にて実行します。
2. インストール画面が表示されるので[次へ]をクリックします。



3. ライセンス条項を承諾後、[はい]をクリックします。

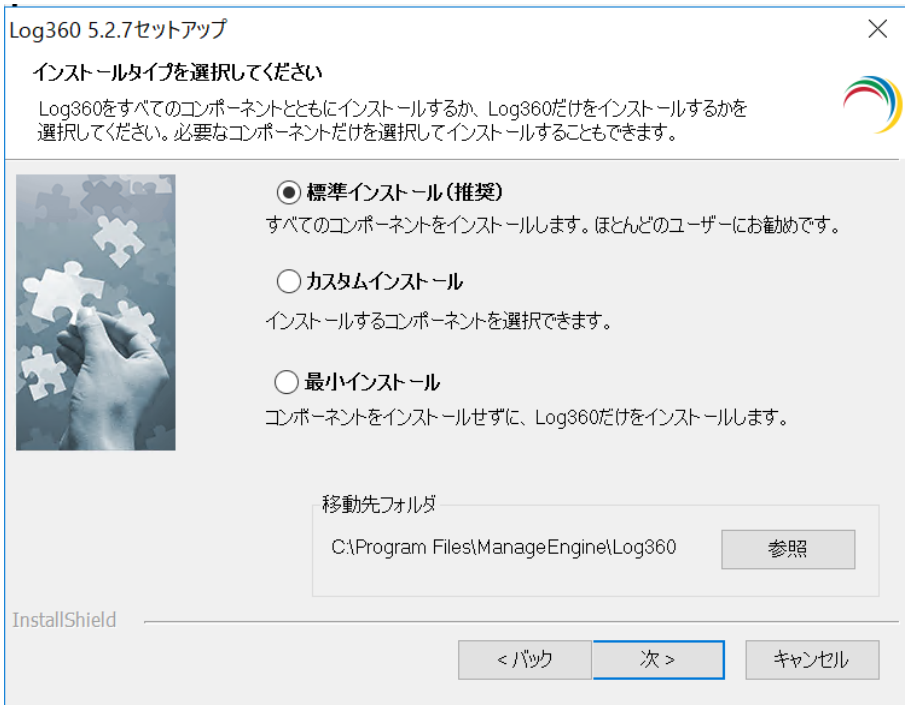


4. インストールディレクトリを選択します。デフォルトは「C:\Program Files\ManageEngine\Log360」です。変更する場合は[参照]をクリックします。また、以下のインストールタイプから1つ選択し、[次へ]をクリックします。

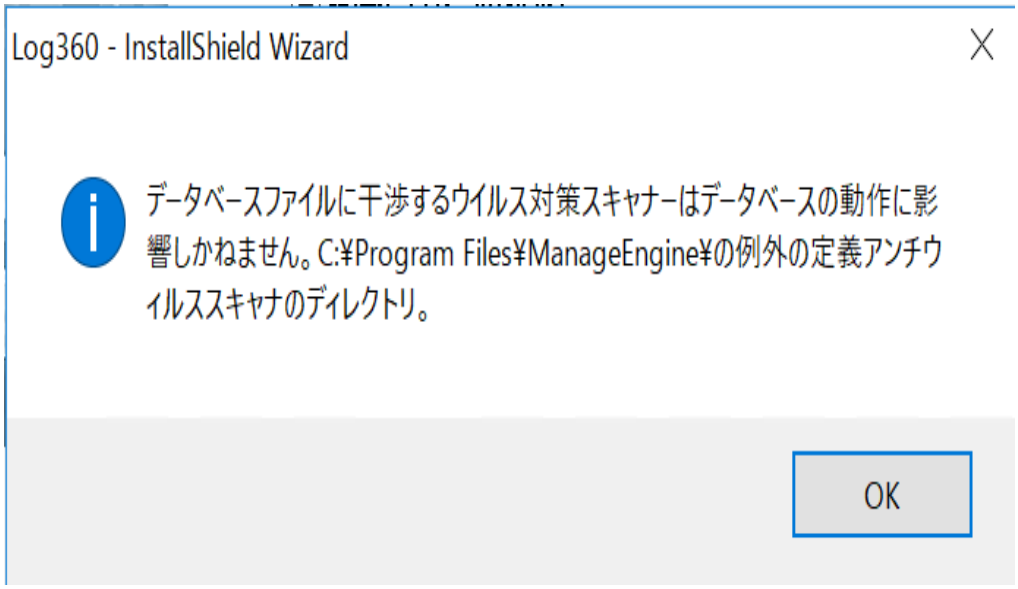
- **標準インストール**
  Log360およびすべてのコンポーネント製品（EventLog Analyzer/ADAudit Plus/M365 Manager Plus/Log360 UEBA）をインストールします。**すべてのサーバーを1つのサーバーにインストールする場合は、本オプションを選択します。**

- **カスタムインストール**
  Log360と併せてインストールするコンポーネント製品を選択できます（[次へ]をクリック後のページで選択します）。

- **最小インストール**
  Log360のみをインストールします。Log360専用のサーバーをご用意いただいている場合、または、コンポーネント製品を既にインストールしている場合に選択します。

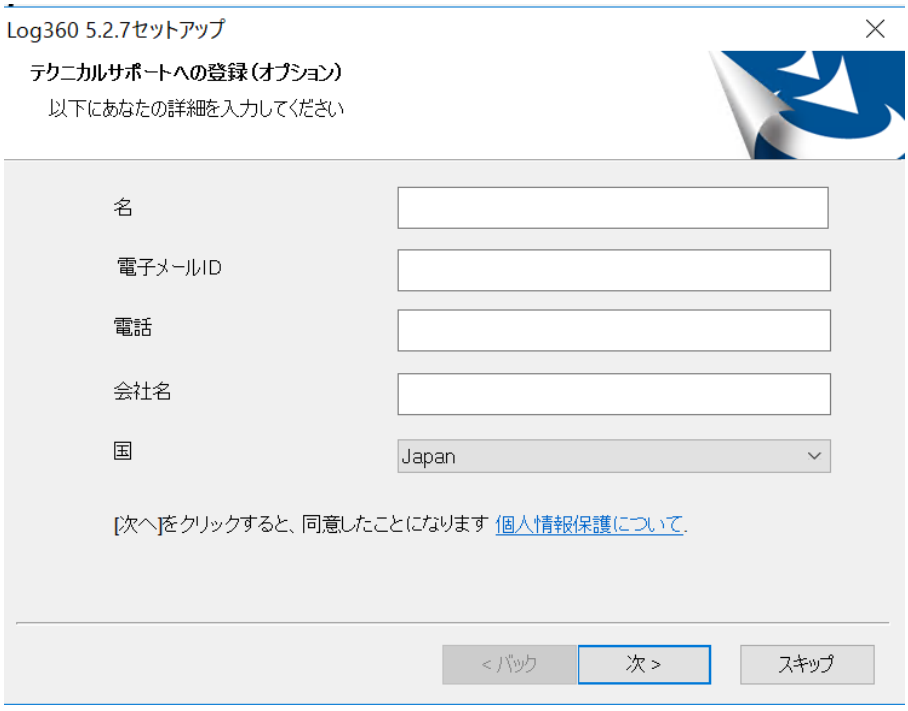


5. アンチウイルスソフトに関する警告画面が表示されますので、[OK]をクリックします。

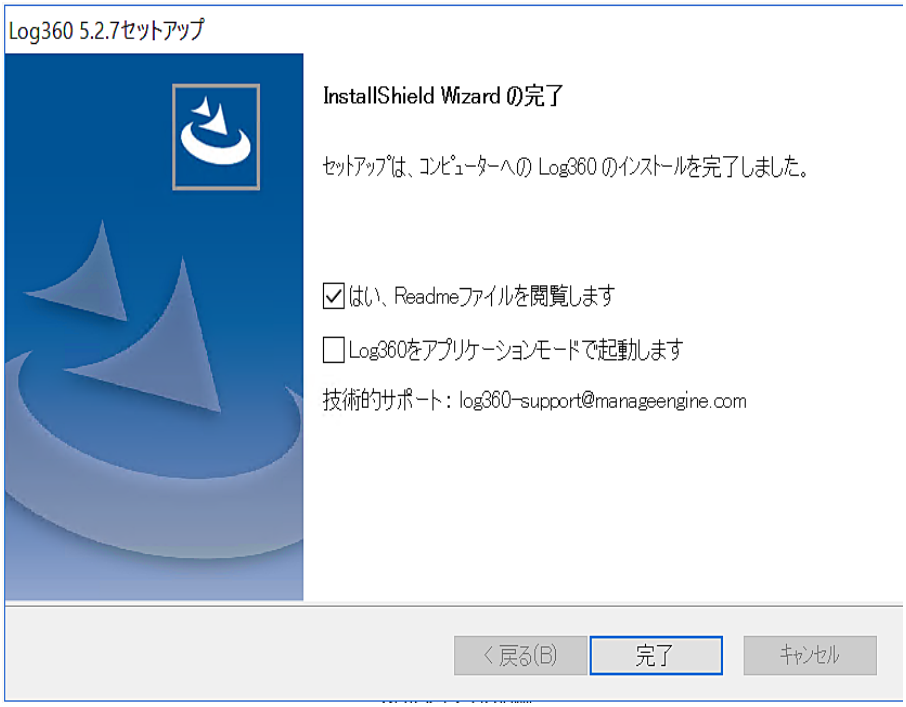


6. Log360をインストールするかの選択を行います。インストールを行う場合は、[次へ]をクリックしてください。インストールが開始されます。

7. お客様情報を入力します（任意）。入力しない場合は[Skip]をクリックします。



8. インストールの完了です。**各チェックボックスの詳細は以下に記載しています。**必要に応じて各チェックを外した後、[完了]をクリックします。



各チェックボックスについて

- [はい、Readmeファイルを閲覧します]: リリースノート情報を記載したページ（英語版）が開きます。
- [Log360をアプリケーションモードで起動します]: Log360がアプリケーション（コンソールモード）として起動します。

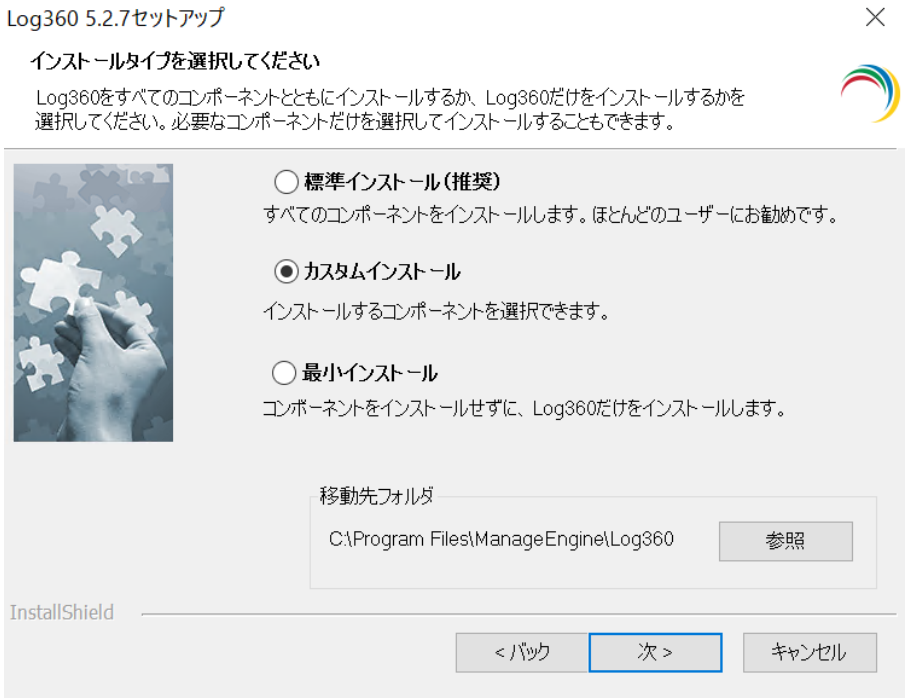
※[Log360をアプリケーションモードで起動します]のチェックを外し、Log360をサービスとしてインストールすることを推奨します。Log360はログ収集・管理ツールであるという製品の性質上、常にバックグラウンドで起動することが推奨されるためです。Log360をサービスとして起動する手順は、[6-1 Log360サービスのインストール・起動手順]をご参照ください。

5-2 製品を2つのサーバーにインストールする場合

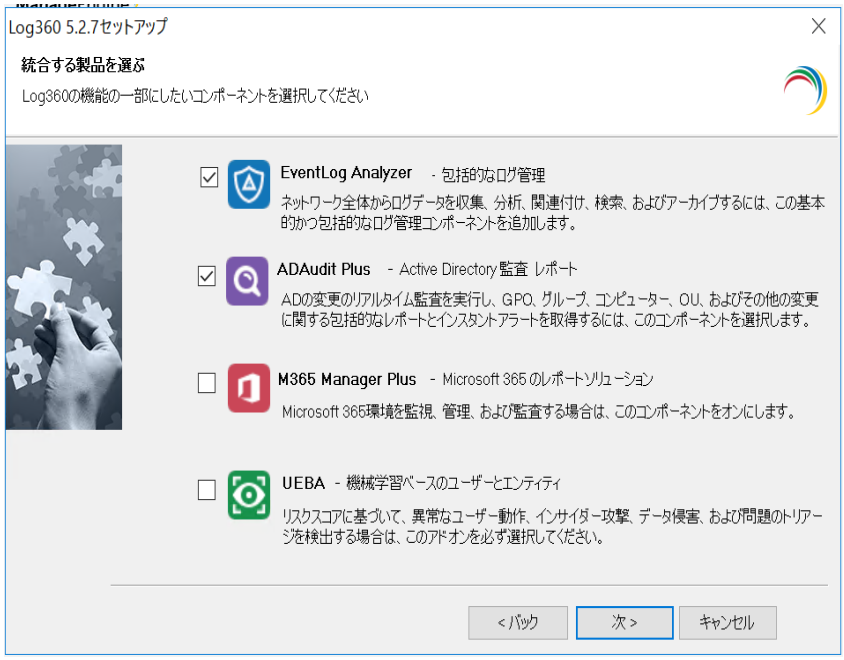
以下のように、製品を2つのサーバーにインストールする場合の手順を記載します。

- **サーバー1**: Log360/EventLog Analyzer/ADAudit Plus
- **サーバー2**: M365 Manager Plus/Log360 UEBA

1. サーバー1上にて、インストール手順[5-1 すべての製品を1つのサーバーにインストールする場合]の手順3まで実施します。
2. 手順4にて、インストールディレクトリを選択後、「**カスタムインストール**」を選択して[次へ]をクリックします。



3. サーバー1にインストールする製品を選択します。今回の例ではEventLog AnalyzerおよびADAudit Plusを選択します。[次へ]をクリックします。



4. インストール手順[5-1 すべての製品を1つのサーバーにインストールする場合]の手順5以降を実施します。
5. [6. 起動と停止]を参照し、Log360を起動します。
6. サーバー2上にて、その他のコンポーネント製品をインストールします。今回の例では、サーバー2上にて、M365 Manager PlusおよびLog360 UEBAをインストールします。各コンポーネント製品のインストーラー（.exeファイル）は以下のページより取得できます。

   【インストーラー取得ページ】
   - EventLog Analyzer
   - ADAudit Plus
   - M365 Manager Plus
   - Log360 UEBA

   インストール手順は各製品のスタートアップガイドをご参照ください。

   【スタートアップガイド】
   - EventLog Analyzer
   - ADAudit Plus
   - M365 Manager Plus
   - Log360 UEBA

7. [8. ログイン方法]を参照し、Log360にログインします。

8. [10-2 製品統合設定]を参照し、サーバー2上にインストールしたコンポーネント製品と統合します。

5-3 Log360のみをインストールする場合

1. サーバー1上にて、インストール手順[5-1 すべての製品を1つのサーバーにインストールする場合]の手順3まで進みます。
2. 手順4にて、インストールディレクトリを選択後、「**最小インストール**」を選択して[次へ]をクリックします。

3. インストール手順[5-1 すべての製品を1つのサーバーにインストールする場合]の手順5以降を実施します。
4. [6. 起動と停止]を参照し、Log360を起動します。
5. [8. ログイン方法]を参照し、Log360にログインします。
6. [10-2 製品統合設定]を参照し、コンポーネント製品と統合します。

6. 起動と停止

6-1 Log360サービスのインストール・起動手順

Log360をアプリケーションとして起動している場合は、アプリケーションを停止してから下記手順を行ってください。アプリケーションを停止する手順は、[6-4 Log360のアプリケーションを停止する手順]をご参照ください。

Log360サービスをインストールする手順は以下のとおりです。

1. [スタート]をクリックします。
2. Log360の中にある「Log360をサービスとしてインストール」をクリックして起動します。
3. Log360が[サービス]に追加されます。
4. [スタート]→[コントロールパネル]→[管理ツール]→[サービス]を開き、[ManageEngine Log360]を選択します。
5.  ボタンまたは「サービスの開始」という文字をクリックすることで、サービスを開始します。

※Log360を起動すると、同じサーバー上で起動する統合済みのコンポーネント製品が自動的に起動します。例えば、インストール手順[5-1 すべての製品を1つのサーバーにインストールする場合]を実施して、すべての製品をインストールした場合、Log360を起動すると、すべてのコンポーネント製品が起動します。

6-2 Log360サービスを停止する手順

[スタート]→[コントロールパネル]→[管理ツール]→[サービス]を開き、[ManageEngine Log360]を選択します。そして■ボタン、あるいは「サービスの停止」という文字をクリックして、サービスを停止してください。

※Log360が停止すると、同じサーバー上で起動する統合済みのコンポーネント製品が自動的に停止します。

6-3 Log360をアプリケーションとして起動する手順

[スタート]→[すべてのプログラム]→[Log360]→[Log360を起動]をクリックします。

6-4 Log360のアプリケーションを停止する手順

[スタート]→[すべてのプログラム]→[Log360]→[Log360を停止]をクリックします。

7. アンインストール手順

Log360をアンインストールする手順は以下のとおりです。

1. Log360を停止します。
2. [スタート]→[Log360]→[Log360をアンインストール]をクリックします。
3. ウィザードに従って、アンインストールを実施します。
4. アンインストール完了後、[完了]ボタンをクリックしてウィザードを閉じます。

8. ログイン方法

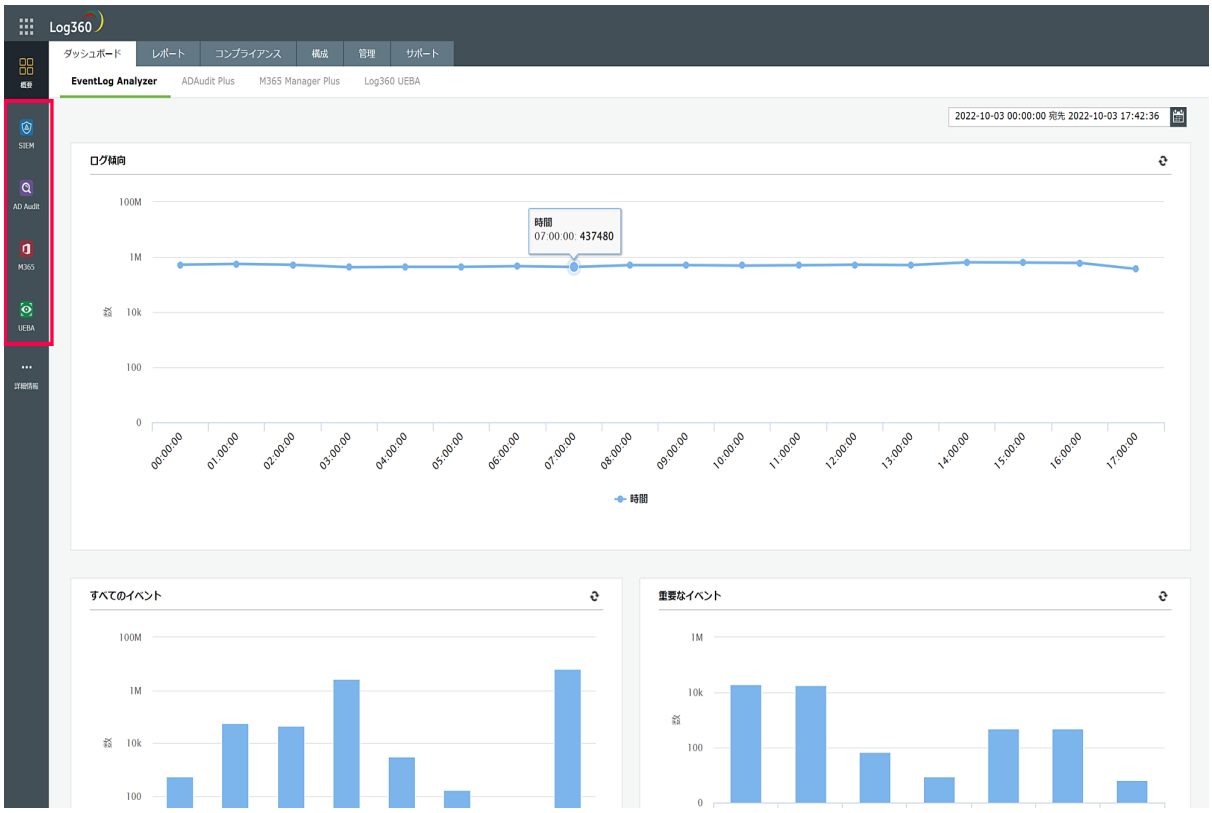
1. Webブラウザーを起動します。
2. アドレスバーに **http://[host_name]:[port_number]** と入力します。

- [host_name]: Log360が起動しているマシンのホスト名またはIPアドレス
- [port_number]: Log360のWebサーバーが使用するポート番号（デフォルトでは**8095**）

例）http://localhost:8095

※SSLを有効化する設定を行った場合は **https://[host_name]:[port_number]** と入力します。

3. ユーザー名とパスワードを入力して、[ログイン]をクリックします（デフォルトのユーザー名とパスワードはともに「admin」です）。
4. 各製品にアクセスするためには、Log360にログイン後、左メニューよりアクセスする製品をクリックします。

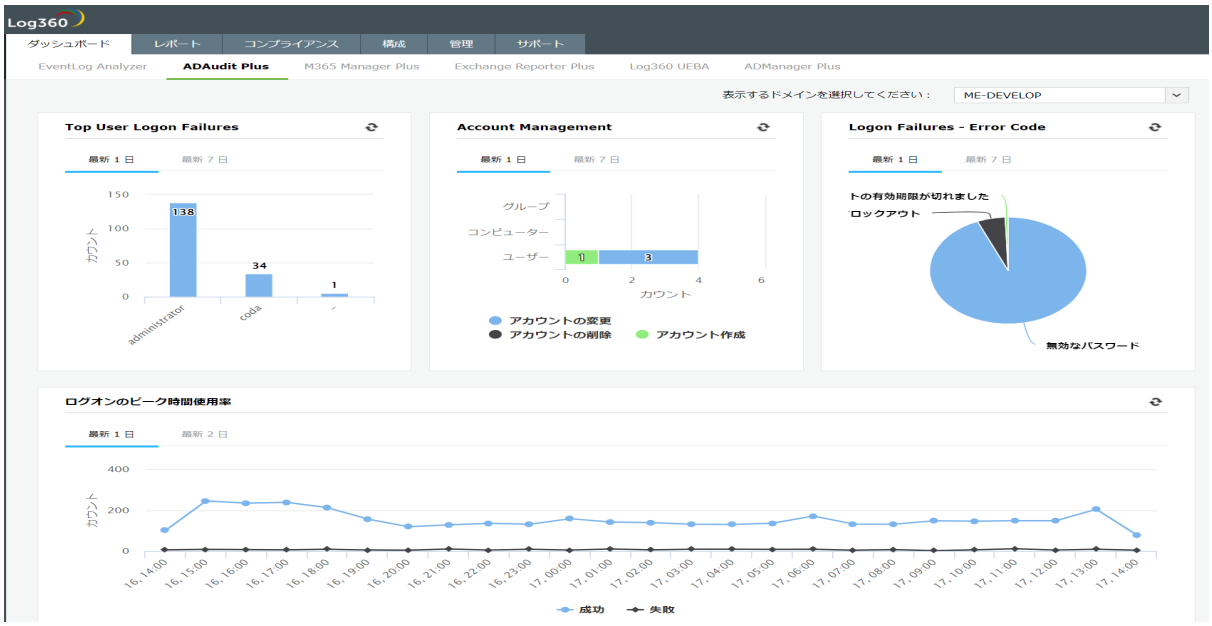


9. 各タブの解説

Log360にログイン後の操作画面を説明します。ヘルプドキュメントを併せてご参照いただけます。

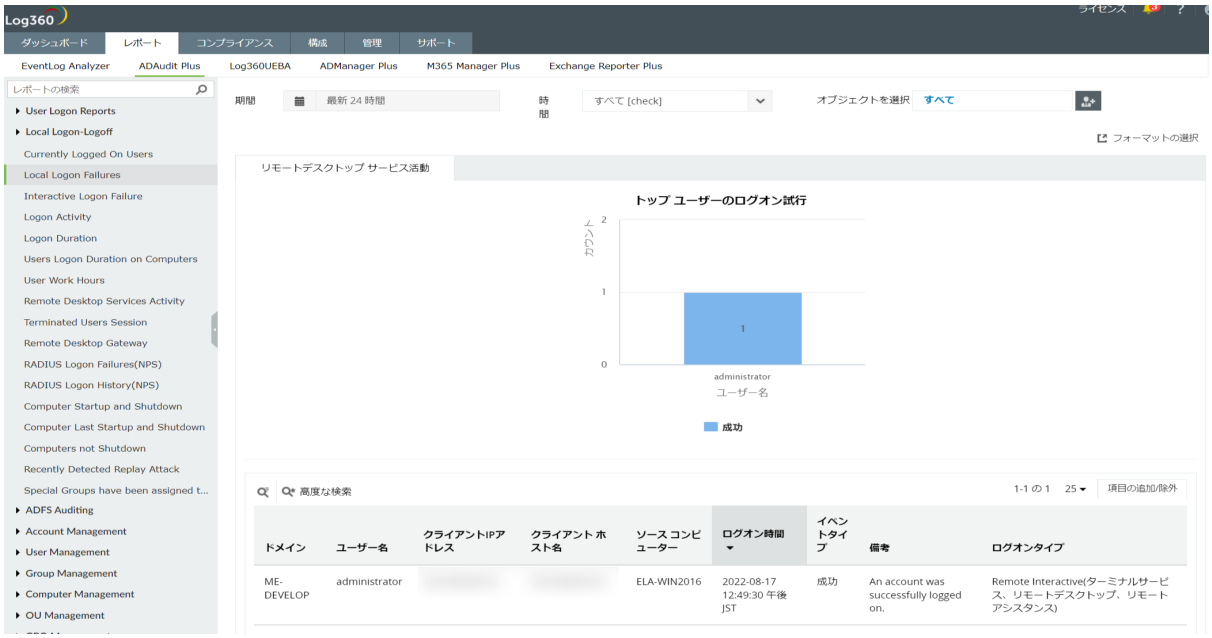
9-1 ダッシュボード

ダッシュボードタブでは、各製品に関する概要レポートが閲覧できます。[ダッシュボード]タブの下に表示されている各製品名をクリックすることで、対象製品内の概要が容易に確認できます。



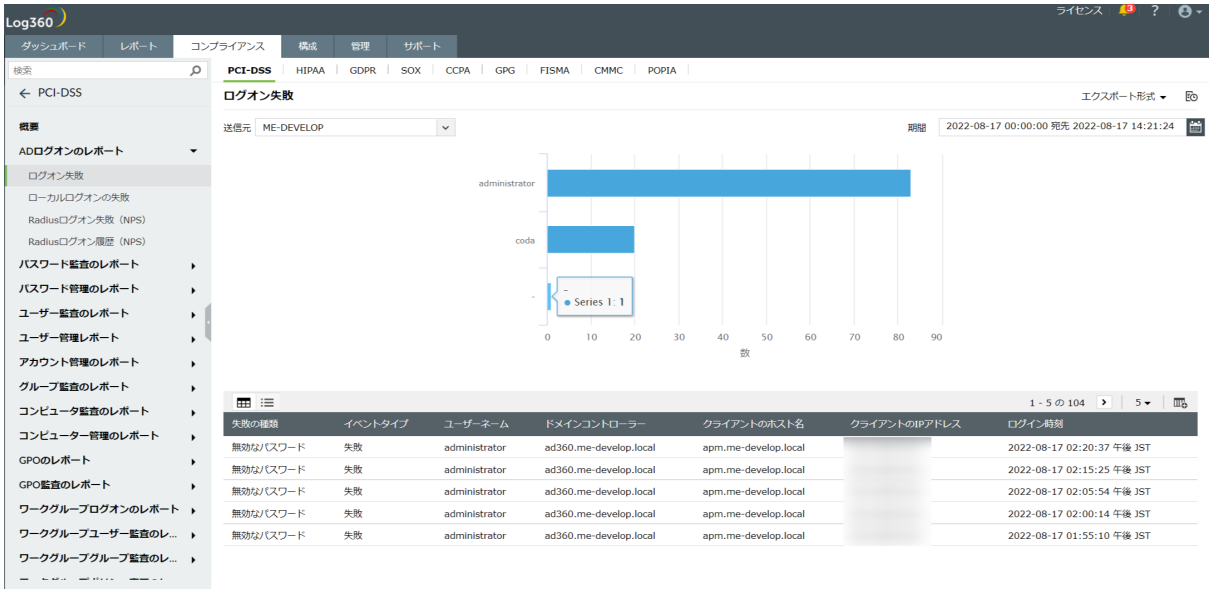
9-2 レポート

レポートタブでは、各製品のレポート機能を一括で閲覧することが可能です。[レポート]タブの下に表示されている各製品名をクリックすることで、対象製品で用意されているレポートを確認できます。下画像はADAudit Plusを選択した場合の画面です。



9-3 コンプライアンス

コンプライアンスタブでは、PCI DSS、SOX法、HIPAA法、GDPRなどの様々な規制法令に適合するレポートを作成できます。レポートはPDF/CSV形式で出力することができ、スケジュールレポートの設定も可能です。

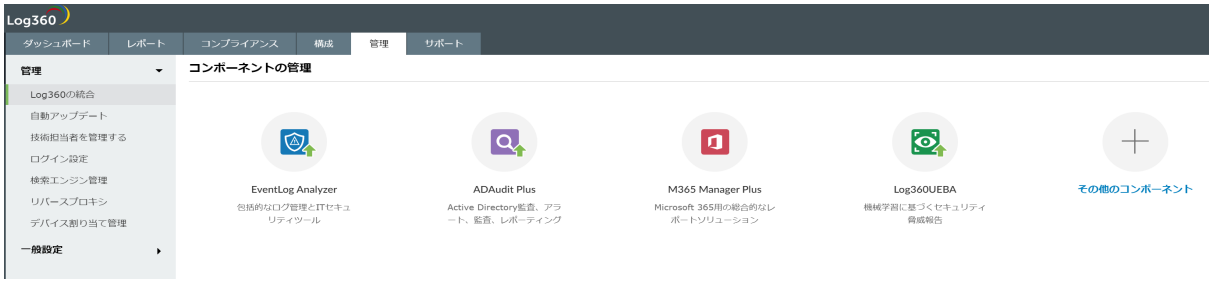


9-4 構成

構成タブでは、監査対象デバイスを管理できます。デバイスの新規追加および監査不要となったデバイスを削除できます。

9-5 管理

管理タブでは、各製品に接続する際のポート番号の設定や製品にログインする際の認証設定（SSO認証や二段階認証）、ディスク空き容量通知設定など、あらゆる設定をカスタマイズできます。



10. システム設定

Log360を使用する際に必要となる設定手順を説明します。

10-1 ドメイン設定

Log360および各コンポーネント製品機能を全て使用可能とするために、**ADAudit PlusまたはEventLog Analyzerにてドメイン設定を実施する必要があります。**

※初めてLog360にログインする際、Log360をインストールしているサーバーがドメインに属している場合は、対象ドメインおよびドメインコントローラーが自動的にディスカバリーされます。しかし、自動的にディスカバリーされた場合も「Domain Admin」以上の権限をもつユーザーの認証情報を改めて登録する必要があります。

ドメイン設定と認証情報の登録はADAudit PlusまたはEventLog Analyzerにて実施してください。いずれかの製品内でドメイン設定後、設定内容が自動的に同期されます。各製品におけるドメイン設定手順はスタートアップガイドをご参照ください。

ドメイン設定手順

- EventLog Analyzer
- ADAudit Plus

10-2 製品統合設定

Log360のUI画面から各コンポーネント製品へのアクセスしたい場合や、コンポーネント製品間でのデータ同期を実施するためには、Log360と統合設定を実施する必要があります。

※[5-1 すべての製品を1つのサーバーにインストールする場合]または[5-2 製品を2つのサーバーにインストールする場合]にてLog360と併せてインストールしたコンポーネント製品は自動的に統合されます。

統合手順は以下のとおりです。

統合手順

1. [管理]→[Log360の統合]をクリックします。
2. 統合設定を実施するコンポーネント製品をクリックします。
3. コンポーネント製品がインストールされているサーバー名/IPアドレス、プロトコル（HTTP/HTTPS）、ポート番号を指定します。
4. [認証情報]にチェックを入れ、製品へログインする際に使用する管理者ユーザー（admin）の認証情報を入力します（デフォルトではadmin/admin）。

10-3 Log360に接続する際のポート番号設定

Log360に接続する際に使用するポート番号は変更可能です（デフォルトは8095）。
変更する場合は、以下の手順を実施してください。

ポート番号変更手順

1. [管理]→[一般設定]→[製品設定]をクリックします。
2. HTTPまたはHTTPSを選択して、ポート番号を入力します。
3. [保存]をクリックします。

※HTTPSを選択する場合は、[キーストアパスワード]の有効化が可能です。
※必要に応じて、[LDAP SSLを有効化]にてドメインを選択してください。

10-4 メールサーバー設定

ライセンス/AMS有効期限や製品ダウンを知らせるメール通知に使用するメールサーバーを設定します。

メールサーバー設定手順

1. [管理]→[システム設定]→[サーバ設定]→[メール設定]タブをクリックします。
2. 以下の情報を入力します。

- サーバー名/IPアドレス: メールサーバーのサーバー名またはIPアドレス
- ポート番号: メールサーバーが使用するポート番号
- 差出人アドレス: メールの差出人となるメールアドレス
- 管理者のメールアドレス: メールの宛先となるメールアドレス
- 保護接続: メールサーバーとの通信がSSLまたはTLS通信となる場合は選択
- 認証: メールサーバーで認証を必要とする場合は、[認証]にチェックを入れ、ユーザー名およびパスワードを入力

3. [通知設定]にて、受信したい通知内容にチェックをいれます。
4. [設定を保存する]をクリックします。

10-5 管理者アカウントのパスワード変更

製品にデフォルトで用意されている管理者アカウント（admin）のログインパスワード（デフォルトパスワード: admin）を変更する手順を説明します。

パスワード変更手順

1. 製品に管理者としてログイン後、画面右上の人型アイコンをクリックします。
2. [パーソナライズ]→[パスワードを変更する]タブをクリックします。
3. [現在のパスワード]に、現在のパスワードを入力します。
4. [新しいパスワード]、[パスワードを確認する]に、新しく設定するパスワードを入力します。
5. [パスワードを変更する]をクリックします。

11. Log360 UEBA

11-1 概要

Log360 UEBA（User and Entity Behavior Analytics : ユーザーおよびエンティティの行動分析）は、ログの分析を通してユーザーやエンティティの行動を学習することで、通常の行動のベースラインを作成します。ベースラインと実際のユーザー/エンティティの行動とを比較し、ユーザー/エンティティごとに「リスクスコア」を算出することで、IT管理者が「異常」な状況を察知しやすくなります。

※リスクスコアは、事前に定義された行動の重み、ベースラインからの逸脱度、逸脱の頻度、逸脱からの経過時間などの要素により、0（リスクなし）～100（リスク最大）で示されます。

11-2 Log360 UEBAを活用するメリット

ネットワーク活動を分析して攻撃を検知するLog360は、既知の攻撃検知に効果を発揮するのに対して、UEBAは機械学習を使用してユーザー/エンティティの異常な行動を検知するので、既存パターンが確立されていない攻撃に対して効果が発揮されます。つまり、Log360にUEBA機能を取り入れることで、より多様な脅威シナリオに対して効果的に対応できるようになります。

11-3 資料の紹介

Log360 UEBAの詳細な情報、活用例をお求めの方はこちらのURLから資料をダウンロードしてください。

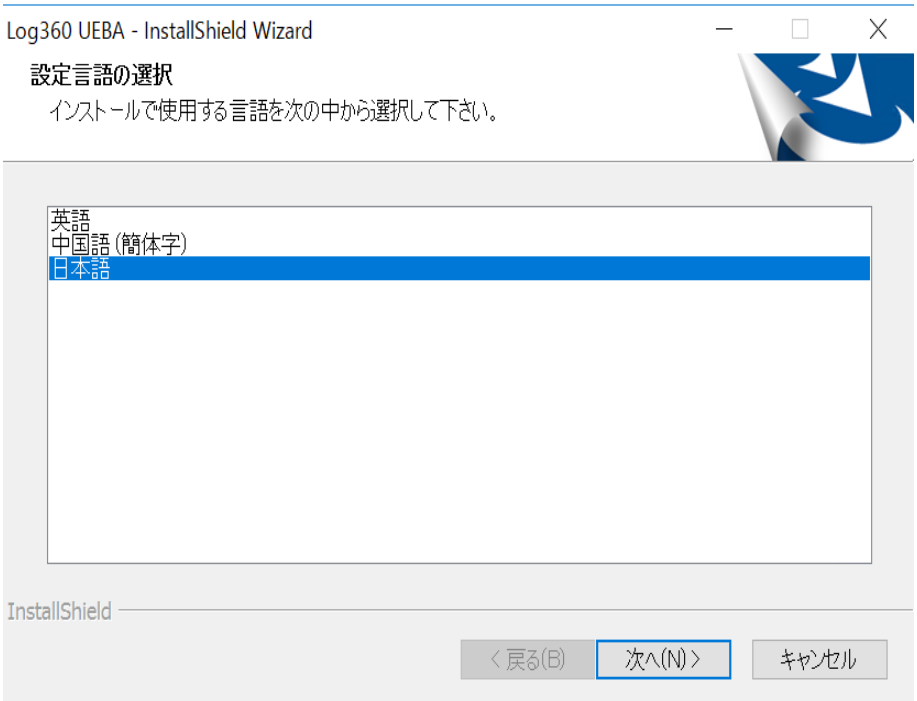
12. Log360 UEBAのインストール手順

Log360 UEBAのインストール手順を説明します。

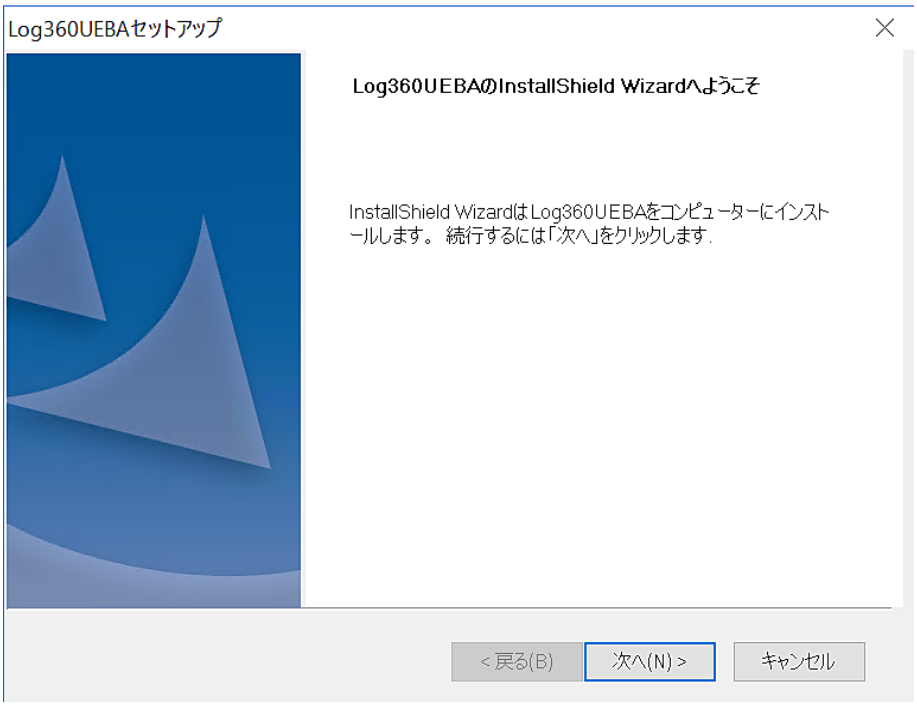
※インストール手順[5-1 すべての製品を1つのサーバーにインストールする場合]を実施して、Log360 UEBAをインストール済みの場合、本手順の実施（Log360 UEBAの単体インストール）は不要です。本手順は、以下のいずれかの手順でLog360をインストールし、Log360 UEBAを単体でインストールする必要がある場合に実施してください。

- [5-2 製品を2つのサーバーにインストールする場合]
- [5-3 Log360のみをインストールする場合]

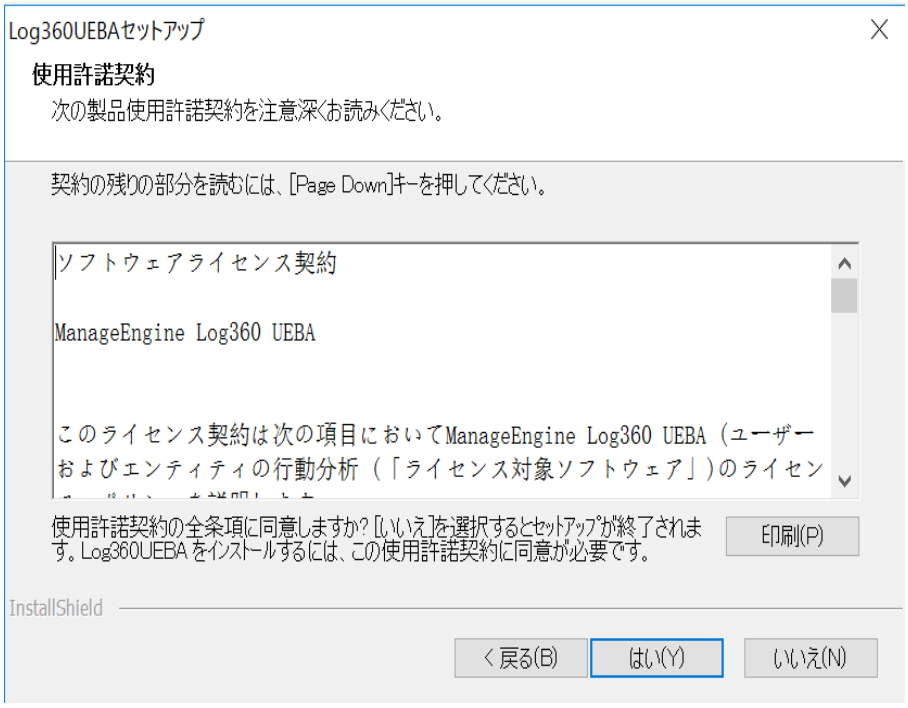
1. 「ManageEngine_Log360UEBA_64bit.exe」を管理者権限にて実行します。使用する言語を選択後、[次へ]クリックします。



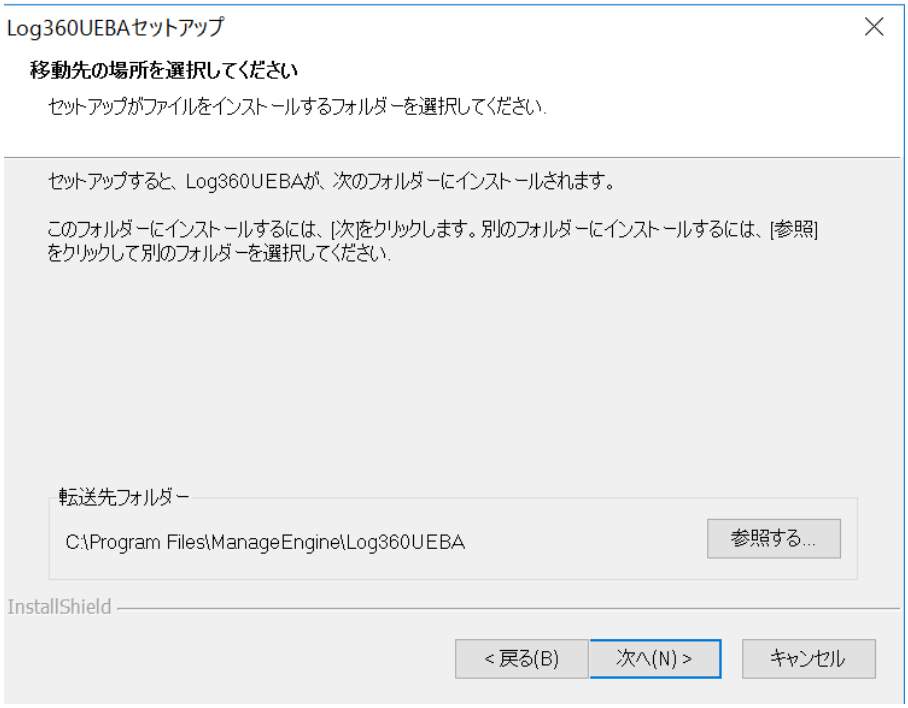
2. インストール画面が表示されるので[次へ]をクリックします。



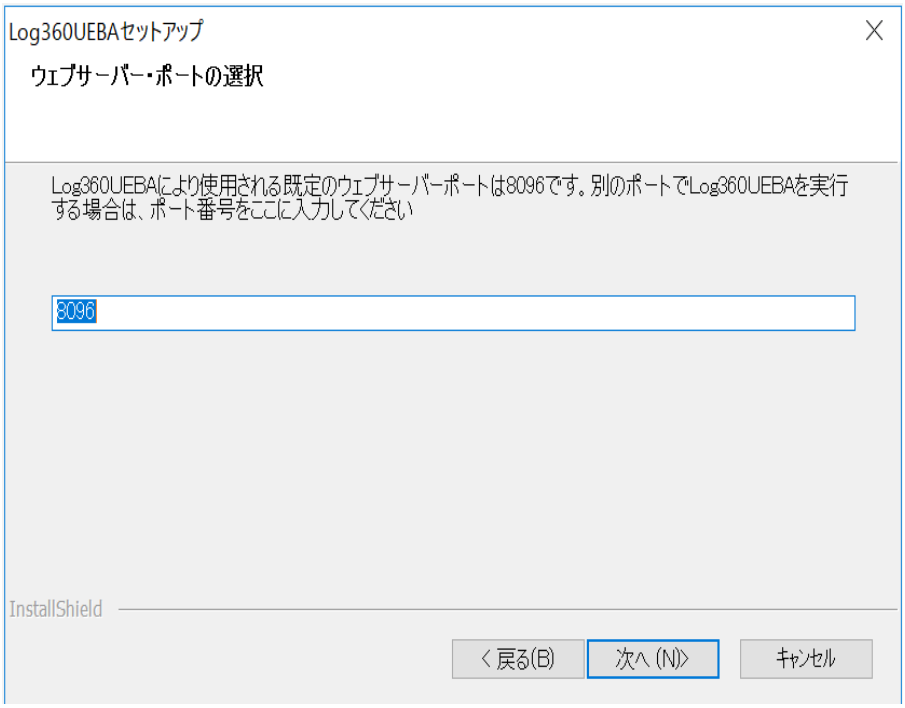
3. ライセンス条項を承諾後、[はい]をクリックします。



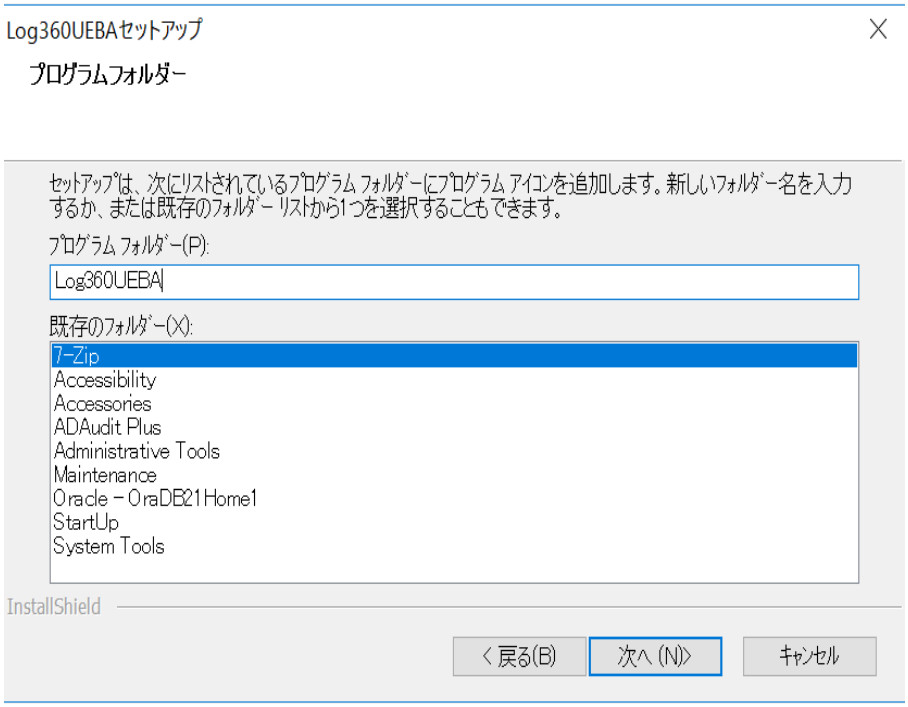
4. インストールディレクトリを選択します。デフォルトは「C:\Program Files\ManageEngine\Log360UEBA」です。変更する場合は[参照する]をクリックします。設定後、[次へ]をクリックします。



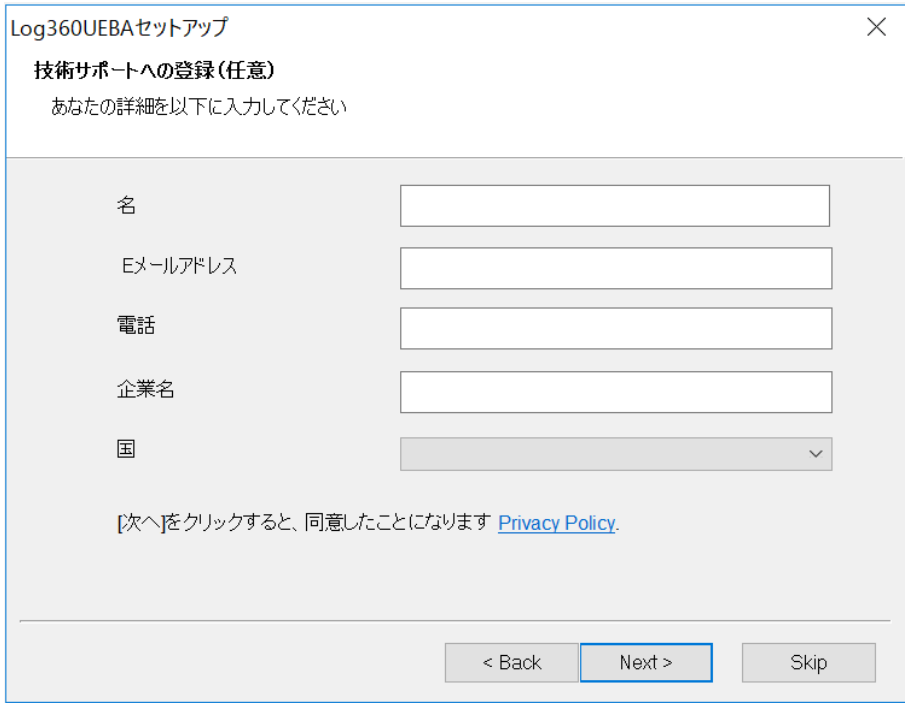
5. Webサーバーのポート番号を入力します。デフォルトでは、**8096**です。入力後、[次へ]をクリックします。



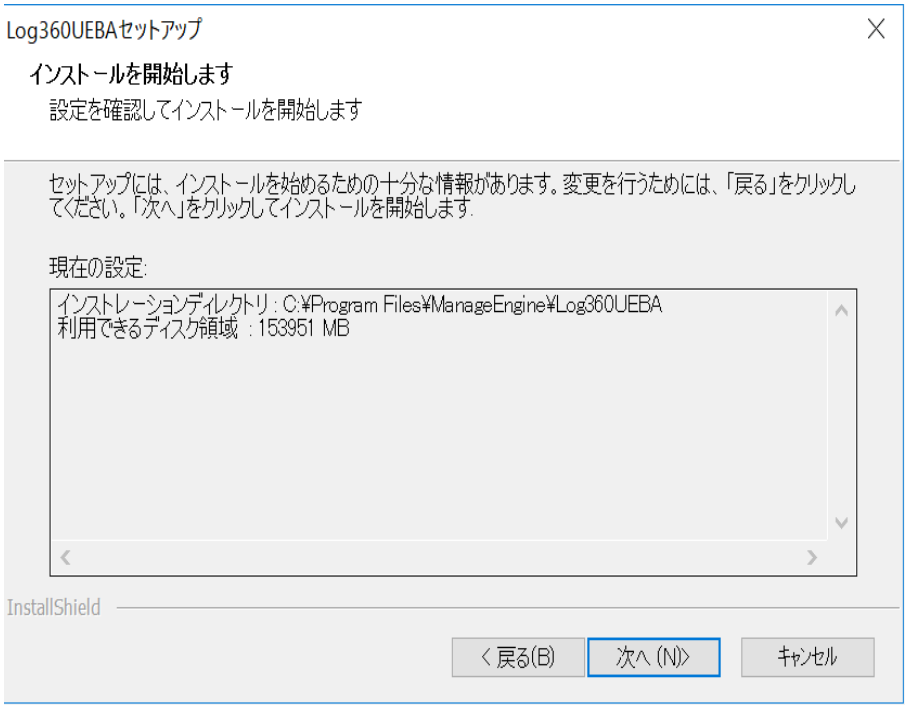
6. プログラムフォルダーにプログラムアイコンを追加します。変更が不要の場合は[次へ]をクリックします。



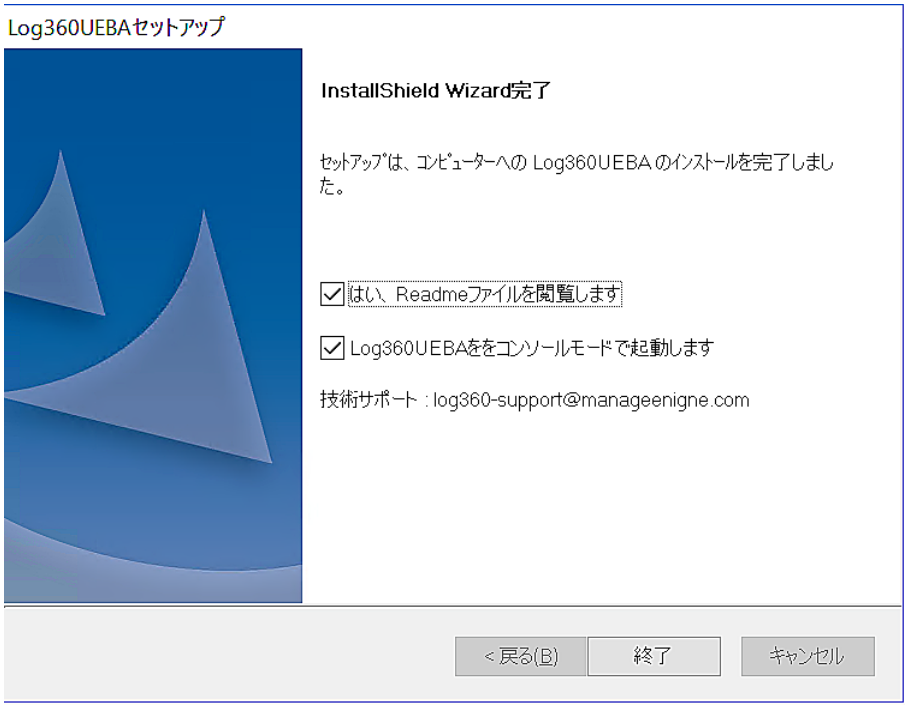
7. お客様情報を入力します（任意）。入力しない場合は[Skip]をクリックします。



8. Log360 UEBAをインストールするか選択します。インストールする場合は[次へ]をクリックします。



9. インストールの完了です。**各チェックボックスの詳細は以下に記載しています。**チェックを必要に応じて選択後、[終了]をクリックします。



各チェックボックスについて

- [はい、Readmeファイルを閲覧します]: リリースノート情報を記載したページ（英語版）が開きます。
- [Log360UEBAをコンソールモードで起動します]: Log360 UEBAがアプリケーション（コンソールモード）として起動します。

※[Log360UEBAをコンソールモードで起動します]のチェックを外し、Log360 UEBAをサービスとしてインストールすることを推奨します。Log360 UEBAは収集したデータを分析するツールであるという製品の性質上、常にバックグラウンドで起動することが推奨されるためです。Log360 UEBAをサービスとして起動する手順は、[13-1 Log360 UEBAサービスのインストール・起動手順]をご参照ください。

13. Log360 UEBAの起動と停止

13-1 Log360 UEBAサービスのインストール・起動手順

Log360 UEBAをアプリケーションとして起動している場合は、アプリケーションを停止してから下記手順を行ってください。アプリケーションを停止する手順は、[13-4 Log360 UEBAのアプリケーションを停止する手順]をご参照ください。

Log360 UEBAサービスをインストールする手順は以下のとおりです。

1. [スタート]をクリックします。
2. Log360 UEBAの中にある「Log360UEBAをサービスとしてインストールします」をクリックして起動します。
3. Log360 UEBAが[サービス]に追加されます。
4. [スタート]→[コントロールパネル]→[管理ツール]→[サービス]を開き、[ManageEngine Log360 UEBA]を選択します。
5.  ボタンまたは「サービスの開始」という文字をクリックすることで、サービスを開始します。

13-2 Log360 UEBAサービスを停止する手順

[スタート]→[コントロールパネル]→[管理ツール]→[サービス]を開き、[ManageEngine Log360 UEBA]を選択します。そして  ボタン、あるいは「サービスの停止」という文字をクリックして、サービスを停止してください。

13-3 Log360 UEBAをアプリケーションとして起動する手順

[スタート]→[すべてのプログラム]→[Log360UEBA]→[Log360UEBAを起動します]をクリックします。

13-4 Log360 UEBAのアプリケーションを停止する手順

[スタート]→[すべてのプログラム]→[Log360UEBA]→[Log360UEBAを停止します]をクリックします。

14. Log360 UEBAのログイン方法

1. Webブラウザーを起動します。
2. アドレスバーに **http://[host_name]:[port_number]** と入力します。

- [host_name]: Log360 UEBAが起動しているマシンのホスト名またはIPアドレス
- [port_number]: Log360 UEBAのWebサーバーが使用するポート番号（デフォルトでは**8096**）

  例）http://localhost:8096

  ※SSLを有効化する設定を行った場合は **https**://[host_name]:[port_number] と入力します。

3. ユーザー名とパスワードを入力して、[サインイン]をクリックします（デフォルトのユーザー名とパスワードはともに「admin」です）。

※Log360 UEBAを使用した監査を開始するためには、以下の条件を満たす必要があります。

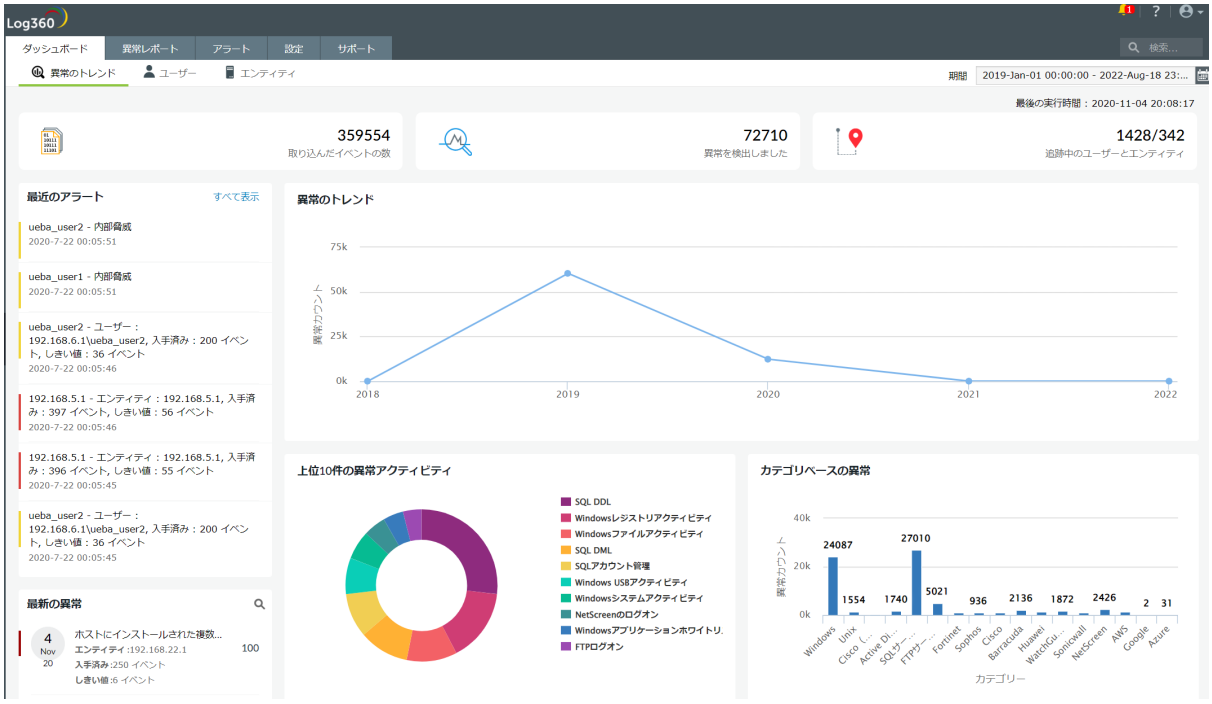
- Log360にて、UEBAとの統合設定が完了していること（統合設定手順は[10-2 製品統合設定]を参照）。
- コンポーネント製品であるEventLog AnalyzerおよびADAudit Plusからのログデータ同期が開始してから24時間経過していること（正確な監査を実施するためには、2週間以上の経過が必要です）。

15. Log360 UEBA 各タブの説明

Log360 UEBAにログイン後の操作画面を説明します。ヘルプドキュメントを合わせてご参照いただけます。

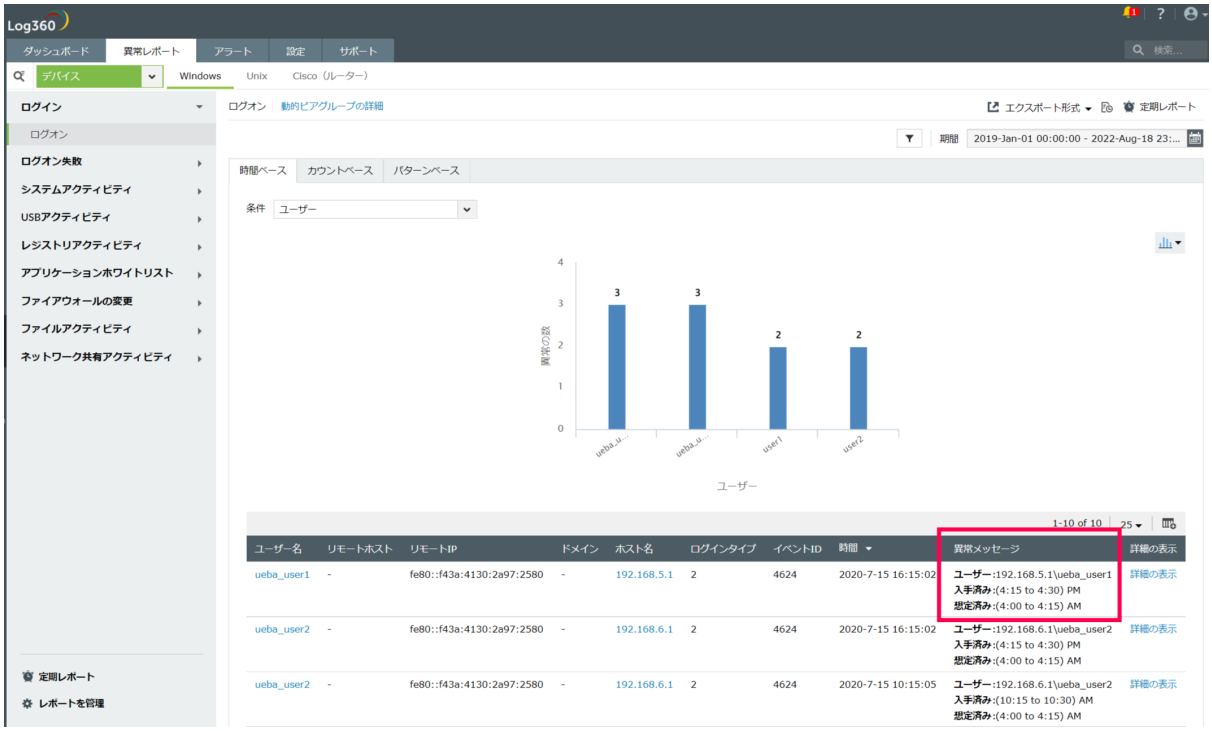
15-1 ダッシュボード

ダッシュボードタブでは、異常のトレンドやユーザー/エンティティのリスクスコアといった概要が表示され、状況を容易に把握することができます。



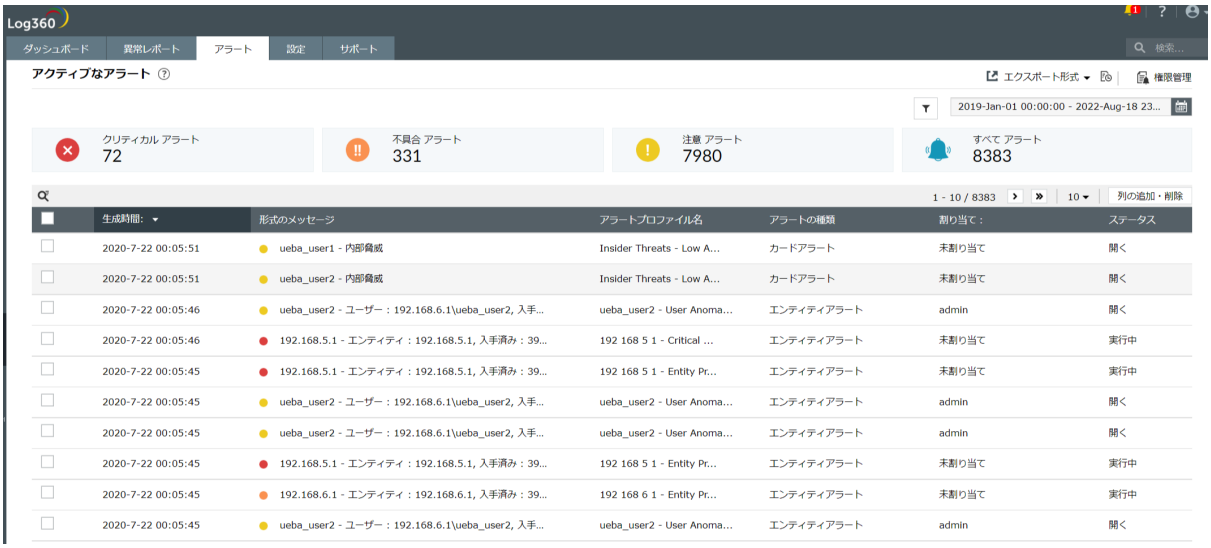
15-2 異常レポート

異常レポートタブでは、管理対象のデバイスやアプリケーションに発生している異常を把握することができます。例えば、以下の画像はログオンのカウントベースに関する異常レポートを示しています。UEBAがこれまでに集積した情報から、対象ユーザーの通常ログオン回数とされる「しきい値」を算出し、そのしきい値を超えた場合に異常と見なされ、以下のレポートが出力されています。



15-3 アラート

アラートタブでは、リスクスコアおよび検出された異常に基づいて発生したすべてのアラートの概要を確認できます。



15-4 設定

設定タブでは、業務時間の設定や製品を操作する技術者の管理、リスクスコアのカスタマイズなどを行うことができます。

リスクスコアカスタマイズの概要

[リスクスコアのカスタマイズ]では、異常値を示すリスクスコアの算出方法をカスタマイズできます。リスクスコアをカスタマイズするためには、それぞれの異常行動に対する「**重み**」と「**減衰係数**」の数値を変更します。

- **重み**
  異常行動に対する重要度を示す値です。値が大きいほど、対象の異常行動が発生した場合にリスクスコアが高くなります。

- **減衰係数**
  リスクスコアが時間とともにどの程度減衰するかを示す値です。値が大きいほど、対象の異常行動が同じ**セッション**内に繰り返し発生すると、リスクスコアが減少しやすくなります。

※**セッション**とは、UEBA内で測定される24時間の単位です。初めてLog360 UEBAを起動するのが午前9時の場合は、当日午前9時～翌日午前9時が1セッションとなります。

16. その他機能の有効化手順

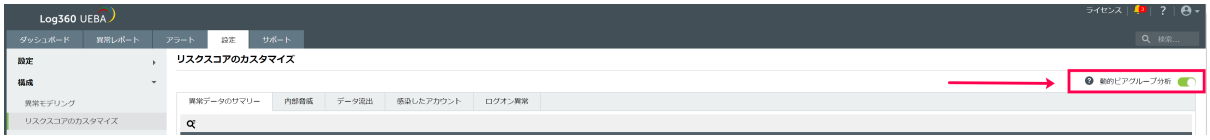
16-1 ユーザーのピアグルーピング

概要

ユーザーを、過去の行動に基づき特定のピアグループに分類することで、より正確なセキュリティ状況の提供が可能となり、誤検知の減少に繋がります。ユーザーは過去の行動に基づき、特定のピアグループに分類されます。ユーザーは複数のピアグループに所属することもあります。ピアグループは、異常の信頼度を計算する際に考慮され、リスクスコアに影響を与えます。

有効化手順

[設定]タブ→[構成]→[リスクスコアのカスタマイズ]をクリック後の画面にて[動的グループ分析]を有効化し、[更新]をクリックしてください。



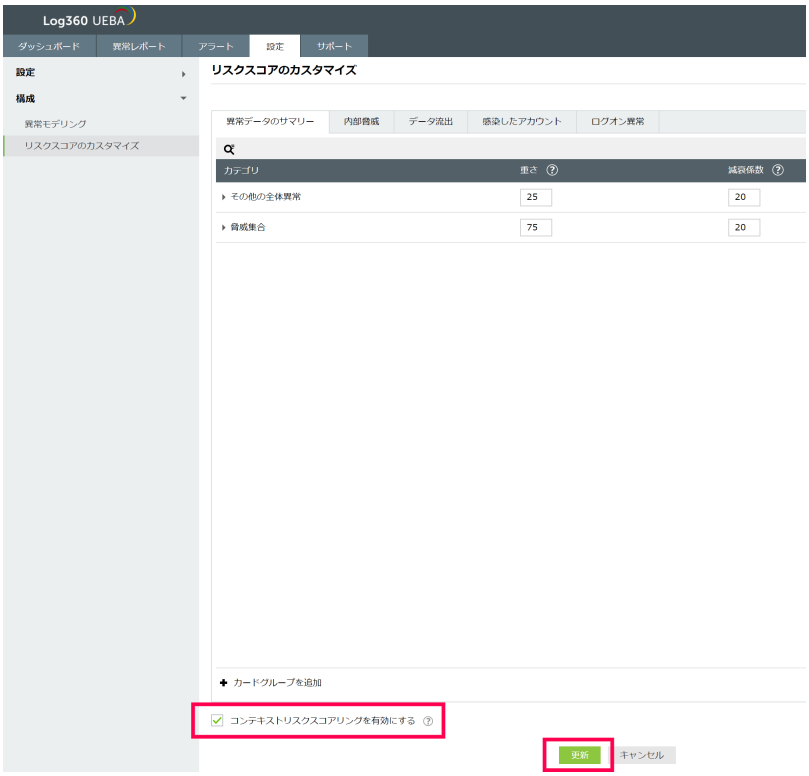
16-2 コンテキストリスクスコアリング

概要

指定された時間範囲の平均およびピークリスクスコアと合わせて、コンテキストリスクスコアを提供します。コンテキストリスクスコアは、指定された時間範囲以降に発生した異常も考慮して計算されたスコアです。

有効化手順

[設定]タブ→[構成]→[リスクスコアのカスタマイズ]をクリック後の画面にて[コンテキストリスクスコアリングを有効にする]を有効化し、[更新]をクリックしてください。



17. お問い合わせ

価格、お見積りなど営業に関するお問い合わせ

https://www.manageengine.jp/purchase/

評価版ご利用中のお客様向け技術サポート

https://www.manageengine.jp/support/trial.html

保守サポート契約締結のお客様向け技術サポート

https://www.manageengine.jp/support/purchased.html

その他製品に関するお問い合わせ

https://www.manageengine.jp/contact.html

会社情報

ゾーホージャパン株式会社 ManageEngine 事業部
〒220-0012 神奈川県横浜市西区みなとみらい3丁目6番1号 みなとみらいセンタービル13階
ホームページ:https://www.manageengine.jp/
Log360製品ページ: https://www.manageengine.jp/products/Log360/